Technology
Arts Sciences
TH Köln

Modulhandbuch IS

IT Security

Master Communication Systems and Networks 2020

Version: 4 | Letzte Änderung: 05.04.2022 17:33 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben | Verantwortlich: Knospe

− Allgemeine Informationen

Anerkannte Lehrveranstaltungen	IS_Knospe
Gültig ab	Wintersemester 2020/21
Modul ist Bestandteil des Studienschwerpunkts	N_S - Networks & Security
Dauer	1 Semester
ECTS	5
Zeugnistext (de)	IT-Sicherheit
Zeugnistext (en)	IT Security
Unterrichtssprache	englisch
abschließende Modulprüfung	Ja

Modulprüfung

Benotet	Ja
Konzept	Schriftliche Prüfung (Klausur)
Frequenz	Jedes Semester

− Allgemeine Informationen

Inhaltliche Voraussetzungen

KRY - Cryptography	Voraussetzungen, Sicherheitsziele und Anwendung kryptographischer Verfahren: Diskrete Strukturen, Wahrscheinlichkeit, Zahlentheorie und Algebra, symmetrische Verschlüsselung, Blockchiffen, Stromchiffren, Hashverfahren, Message Authentication Codes, Erzeugung von Pseudozufallszahlen, asymmetrische Verschlüsselung, Digitale Signaturen, Schlüsselvereinbarung, Hybride Verschlüsselung, Elliptische-Kurven-Kryptographie.

Handlungsfelder

Algorithmen, Protokolle, Schaltungen und kommunikationstechnische Systeme unter interdisziplinären Bedingungen entwickeln und testen

Wissenschaftlich arbeiten und wissenschaftliche Erkenntnisse anwenden und erweitern

Learning Outcomes

ID	Learning Outcome
LO1	Was: Das Modul vertieft zentrale Konzepte und Verfahren der IT-Sicherheit, die für den Entwurf, die Analyse und die Implementierung von kommunikationstechnischen Systemen vor dem Hintergrund von diversen SIcherheitsbedrohungen eine wichtige Rolle spielen (K. 1, 2, 3). Die Studierenden lernen die Analyse von Systemen in Bezug auf Sicherheitsanforderungen (K. 2 und K. 4). Die Studierenden beschaffen sich hierfür Informationen aus unterschiedlichen Quellen (K. 7) und wenden wissenschaftliche Methoden an (K. 16). Ethische und gesellschaftliche Grundwerte spielen im Zusammenhang mit Angriffen gegen die Sicherheit von Daten und Systemen eine wichtige Rolle (K. 21). Womit: Der Dozent/die Dozentin vermittelt Wissen und Basisfertigkeiten in der Vorlesung. In der Übung bearbeiten die Studierenden unter Anleitung Aufgaben. Im Praktikum werden konkrete Probleme und Fragestellungen der IT-Sicherheit bearbeitet. Wozu: Im Profil Network and Security des Studiengangs werden vertiefte Kenntnisse der IT-Sicherheit und der Cyber-Sicherheit benötigt. Sie sind ein anerkannter und notwendiger Teil der Qualifikation für Fach- und Führungsaufgaben in diesem Bereich. Bei der Entwicklung von kommunikationstechnischen Systemen spielen Fragen der IT-Sicherheit heute eine wichtige Rolle (HF1).

Kompetenzen

Kompetenz	Ausprägung
kommunikationstechnische Systeme und Prozesse entwerfen	diese Kompetenz wird vermittelt
kommunikationstechnische Systeme und Prozesse analysieren	diese Kompetenz wird vermittelt
kommunikationstechnische Systeme und Prozesse realisieren	diese Kompetenz wird vermittelt
Informationen und wissenschaftliche Literatur beschaffen, analysieren, verstehen und auswerten	diese Kompetenz wird vermittelt
Wissenschaftliche Methoden anwenden	diese Kompetenz wird vermittelt
Gesellschaftliche und ethische Grundwerte anwenden	diese Kompetenz wird vermittelt

Vorlesung / Übungen

Typ	Vorlesung / Übungen
Separate Prüfung	Nein
Exemplarische inhaltliche Operationalisierung	Introduction to IT Security - Standards and Guidelines - Taxonomy - Security Objectives, Vulnerabilities, Threats, Risk, Attacks, Security Controls Authentication and Key Establishment - Authentication Protocols - Key Exchange - Kerberos - Public Key Infrastructures - Passwords and their Vulnerabilities - Security Token Access Control - Authentication, Authorization, Auditing - Discretionary and Mandatory Access Control - Access Matrix, Unix ACL - Role-Based Access Control - Multi-Level Security, Bell-LaPadula Model Network Security - Threat Model - LAN and WLAN Security - IP Security, IPsec - TCP Security, TLS, SSH - Virtual Private Networks - IDS and IPS - Firewalls and UTM - DNS Security Software Security - Safety and Security - Software Vulnerabilities - Web Security Security Management - Information Security Management System - Security Standards ISO 27001, ISO 27002, BSI Grundschutz - Privacy Regulations

Praktikum

Typ	Praktikum
Separate Prüfung	Ja

Separate Prüfung

Benotet	Nein
Frequenz	Einmal im Jahr

Exemplarische inhaltliche Operationalisierung	- Generation of key pairs, certificates and setting up a public-key infrastructure (PKI). - Implementation of a secure socket connection and analysis of a TLS handshake. - Implementation and analysis of a VPN. - Penetration testing of web applications using open source tools. - Perform SQL injection, XSS and CSRF attacks against test systems. - Reconnaissance, exploitation and infiltration in a lab environment. - Interpret DNS and HTTP data to analyze an attack.

Voraussetzung für Teilnahme an Modulprüfung	Ja
Konzept	Individuelle Lernstandsrückmeldung und Testat